

# ON THE MAXIMUM ORDER OF NILPOTENT TRANSITIVE PERMUTATION GROUPS

ELEONORA CRESTANI AND PABLO SPIGA

**ABSTRACT.** Given two positive integers  $n$  and  $c$ , we determine an upper bound, as a function of  $n$  and  $c$ , for the maximum order of a finite nilpotent transitive group of degree  $n$  and nilpotency class at most  $c$ .

## 1. INTRODUCTION

It is well-known and easy to show that every transitive abelian group of degree  $n$  acts regularly, and hence has order equal to  $n$ . This behaviour is peculiar to abelian groups, but one might wonder, if minded so, whether there is any relationship among the order  $|G|$ , the degree  $n$  and the nilpotency class  $c$  of a nilpotent transitive permutation group  $G$ . Broadly speaking, in this paper we uncover this relationship.

Clearly, when  $G$  is non-abelian,  $|G|$  is not uniquely determined by  $n$  and  $c$ : for instance, the symmetric group  $\text{Sym}(16)$  contains nilpotent transitive groups of class 3 and order  $2^\ell$ , with  $\ell$  ranging from 4 to 10, see [2]. Therefore, it is natural to look for lower and upper bounds for  $|G|$ , as functions of  $n$  and  $c$ . Actually, in this paper, we are only concerned with upper bounds for  $|G|$  (as functions of  $n$  and  $c$ ). We have two reasons to make this choice. First, our motivation for this work is spurred by the proofs of [7, Theorem 2] and [9, Theorem 1.3]. In these papers the authors are interested in bounding the order of the vertex-stabilisers of certain finite vertex-transitive graphs, and at a critical juncture they need to estimate the maximum order of a transitive  $p$ -group of degree  $n$  and nilpotency class at most 3. In both papers this problem was by-passed using the rigid structure of the Sylow subgroups of the vertex-stabilisers under consideration, however this resulted in very technical arguments and (in our opinion) in an artificial detour. In particular, our work (specifically Theorem 1.5 below) can be used to simplify the proofs of [7, Theorem 2] and [9, Theorem 1.3]. Second, the function determining the minimum order of a nilpotent transitive group of degree  $n$  and nilpotency class  $c$  seems to be rather irregular and dramatically influenced by the prime factorisation of  $n$ . Moreover, when  $n = p^k$  for some prime number  $p$  and some  $k \geq 1$ , Remark 2.5 suggests that a lower bound for  $|G|$  becomes an interesting and meaningful problem only when  $c$  is large compared to  $k$ .

**Definition 1.1.** Let  $n$  and  $c$  be positive integers. We define

$$F_{\text{Nil}}(n, c) := \max\{|G| \mid G \text{ nilpotent transitive permutation group of degree } n \text{ and nilpotency class at most } c\}.$$

---

2010 *Mathematics Subject Classification.* 20B05, 20D10, 20D15.

*Key words and phrases.* finite transitive groups, nilpotency class.

Address correspondence to P. Spiga, E-mail: pablo.spiga@unimib.it.

Clearly,  $F_{\text{Nil}}(n, 1) = n$ .

Our choice of allowing nilpotent transitive permutation groups of nilpotency class at most  $c$  (rather than equal to  $c$ ) in Definition 1.1 is aesthetic: it makes the statements of our main results clearer and, in our view, more natural.

Our first result reduces the problem of computing  $F_{\text{Nil}}(n, c)$  to the analogous problem on prime power degrees.

**Theorem 1.2.** *Let  $n$  and  $c$  be positive integers and let  $n = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$  be the prime factorisation of  $n$ , with  $p_1, \dots, p_\ell$  distinct prime numbers and  $\alpha_1, \dots, \alpha_\ell \geq 1$ . Then*

$$F_{\text{Nil}}(n, c) = \prod_{i=1}^{\ell} F_{\text{Nil}}(p_i^{\alpha_i}, c).$$

In view of Theorem 1.2, we need only to consider the case when  $n$  is a prime power. Our second result gives an explicit formula for  $F_{\text{Nil}}(p^k, 2)$  and a description of the nilpotent transitive groups  $G$  of degree  $p^k$ , nilpotency class at most 2 and order  $F_{\text{Nil}}(p^k, 2)$ .

**Theorem 1.3.** *Let  $p$  be a prime number and let  $k \geq 1$ . We have*

$$\log_p(F_{\text{Nil}}(p^k, 2)) = k + \left\lfloor \frac{k}{2} \right\rfloor \left\lceil \frac{k}{2} \right\rceil.$$

Moreover, if  $G$  is a nilpotent transitive group of degree  $p^k$ , nilpotency class at most 2 and order  $F_{\text{Nil}}(p^k, 2)$ , then  $G$  is permutation isomorphic to one of the groups in Example 3.2.

In this opening section we do not introduce the groups in Example 3.2 because a precise definition would take us too far astray. We refer also to Example 3.1 and Remarks 3.3 and 3.4 for more information on the groups in Example 3.2.

**Definition 1.4.** Let  $k$  and  $c$  be positive integers. We let

$$F(k, c) := \max \left( \sum_{i=1}^c a_i \left( \frac{\left( \sum_{j=1}^{i-1} a_j \right)^i - 1}{\left( \sum_{j=1}^{i-1} a_j \right) - 1} \right) \mid a_1, \dots, a_c \in \mathbb{N}, k = \sum_{j=1}^c a_j \right),$$

With the help of MAGMA, we have tabulated  $F(k, c)$  in Table 1, for  $c \leq 4$ .

In Proposition 4.1, we show that, when  $c$  is fixed,

$$F(k, c) = \frac{(c-1)^{c-1} k^c}{c^c} + o(k^{c-1}).$$

Hence, for  $c$  fixed,  $F(k, c)$  can be thought of as a polynomial in  $\mathbb{Q}[k]$  of degree  $c$  and having leading coefficient

$$\frac{(c-1)^{c-1}}{c^c} = \frac{1}{c-1} \left( 1 - \frac{1}{c} \right)^c.$$

In particular, the leading coefficient of  $(c-1)F(k, c)$  is asymptotic to the ubiquitous  $1/e$ .

**Theorem 1.5.** *Let  $p$  be a prime number, let  $k \geq 1$  and let  $F(k, c)$  be as in Definition 1.4. Then  $\log_p(F_{\text{Nil}}(p^k, c)) \leq F(k, c)$ .*

In Proposition 4.2, we prove that the upper bound in Theorem 1.5 is (for  $c$  small compared to  $k$ ) not far from best possible. Specifically, we show that  $\log_p(F_{\text{Nil}}(p^k, c))$  is bounded from below by a polynomial in  $k$  of degree  $c$ .

We conclude this introductory section referring to the beautiful article [6]. Here, Pálffy surveys the known estimates of the form “ $|G| \leq f(n)$ ” for (not necessarily transitive) permutation groups  $G$  of degree  $n$ , where the function  $f$  depends on whether the group  $G$  is abelian, nilpotent or soluble. See [6, Table 1] for a comprehensive table of classical results, mostly taken from [3]. The investigation of Pálffy differs from ours in at least two important facts. First, we are only concerned with transitive groups. Second (and more importantly), our estimates are functions of both the degree and the nilpotency class. For instance, from [6, Table 1] we infer that a transitive nilpotent group  $G$  of degree  $n$  has order at most  $2^{n-1}$ , which is exponential in  $n$ . Theorem 1.5 reveals that, once the nilpotency class of  $G$  is fixed,  $|G|$  is poly-logarithmic in  $n$ .

$c$	$k$	$F(k, c)$
1	any	$k$
2	any	$\lfloor \frac{k}{2} \rfloor \lceil \frac{k}{2} \rceil + k$
3	$k \equiv 0 \pmod 3$	$\frac{4}{27}k^3 + \frac{1}{3}k^2 + k$
3	$k \equiv 1 \pmod 3$	$\frac{4}{27}k^3 + \frac{1}{3}k^2 + \frac{8}{9}k - \frac{10}{27}$
3	$k \equiv 2 \pmod 3$	$\frac{4}{27}k^3 + \frac{1}{3}k^2 + \frac{8}{9}k - \frac{8}{27}$
4	2	5
4	6	188
4	$k \equiv 0 \pmod 4$	$\frac{27}{256}k^4 + \frac{13}{64}k^3 + \frac{3}{8}k^2 + k$
4	$k \equiv 1 \pmod 4$	$\frac{27}{256}k^4 + \frac{13}{64}k^3 + \frac{41}{128}k^2 + \frac{53}{64}k - \frac{117}{256}$
4	$k \equiv 2 \pmod 4, k > 6$	$\frac{27}{256}k^4 + \frac{13}{64}k^3 + \frac{1}{8}k^2 + \frac{7}{16}k - \frac{11}{16}$
4	$k \equiv 3 \pmod 4$	$\frac{27}{256}k^4 + \frac{13}{64}k^3 + \frac{37}{128}k^2 + \frac{57}{64}k - \frac{77}{256}$

TABLE 1.  $F(k, c)$ , for  $c \leq 4$ 

**1.1. Notation.** Our notation is standard. Given a finite nilpotent group  $G$ , we denote by  $\gamma_i(G)$  the  $i^{\text{th}}$ -term of the lower central series of  $G$ , and by abuse of notation, we write  $\gamma_1(G) = G$ . As usual  $\mathbf{Z}(G)$  denotes the centre of  $G$  and  $\mathbf{Z}_i(G)$  denotes the  $i^{\text{th}}$ -term of the upper central series of  $G$ . Given two subsets  $X$  and  $Y$  of  $G$ , the commutator subgroup of  $X$  and  $Y$  is denoted by  $[X, Y] := \langle [x, y] \mid x \in X, y \in Y \rangle$ , and the centraliser of  $X$  in  $G$  by  $\mathbf{C}_G(X)$ .

If  $G$  is a permutation group on  $\Omega$  and  $\omega \in \Omega$ , then we denote by  $G_\omega$  the stabiliser in  $G$  of the point  $\omega$ .

**1.2. Structure of the paper.** In Section 2 we prove Theorem 1.2 (which is an easy observation). We prove Theorem 1.3 in Section 3 and Theorem 1.5 in Section 4.

**1.3. Acknowledgements.** The ideas that gave rise to this work owe very much to some conversations that the second author had with Gabriel Verret during his visit at the University of Western Australia in 2014. He thanks UWA for the warm hospitality, Gab for the constant encouragement and Gordon Royle for sharing his wisdom on caramelised onion on lamb chops.

## 2. PRELIMINARIES

Let  $H$  and  $K$  be transitive groups on  $\Delta$  and  $\Lambda$ , respectively. The direct product  $H \times K$  acts transitively on the set  $\Delta \times \Lambda$  by setting  $(\delta, \lambda)^{(h, k)} = (\delta^h, \lambda^k)$ , for each  $(\delta, \lambda) \in \Delta \times \Lambda$  and each  $(h, k) \in H \times K$ . We refer to this faithful action of  $H \times K$  as the *natural product action*.

Let  $n$  be a positive integer and let  $n = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$  be the prime factorisation of  $n$ , with  $p_1, \dots, p_\ell$  prime numbers and  $\alpha_1, \dots, \alpha_\ell \geq 1$ . Let  $G$  be a nilpotent transitive group on the set  $\Omega$  of cardinality  $n$  and let  $\omega \in \Omega$ . Let  $R$  be a Sylow  $r$ -subgroup of  $G$  with  $r \nmid n$ . As  $|G : G_\omega| = n$  is coprime to  $r$ , by Sylow's theorems  $R$  is conjugate to a subgroup of  $G_\omega$ . Since  $G$  is nilpotent, we have  $R \trianglelefteq G$  and, since  $G_\omega$  is core-free in  $G$ , we have  $R = 1$ . This shows that  $G = P_1 \times \cdots \times P_\ell$ , where  $P_i$  is the Sylow  $p_i$ -subgroup of  $G$  for each  $i \in \{1, \dots, \ell\}$ . Write  $G_\omega = Q_1 \times \cdots \times Q_\ell$ , where  $Q_i := (P_i)_\omega$  is the Sylow  $p_i$ -subgroup of  $G_\omega$ . We let  $\Omega_i$  denote the  $P_i$ -orbit containing  $\omega$ , that is,  $\Omega_i := \omega^{P_i} = \{\omega^g \mid g \in P_i\}$ .

**Proposition 2.1.** *Assume the notation we have established above. The action of  $G$  on  $\Omega$  is permutation isomorphic to the natural product action of  $G = P_1 \times \cdots \times P_\ell$  on  $\Omega_1 \times \cdots \times \Omega_\ell$ .*

*Proof.* Observe that  $|\Omega_i| = |P_i : (P_i)_\omega| = |P_i : Q_i| = p_i^{\alpha_i}$  and hence  $|\Omega| = \prod_{i=1}^\ell |\Omega_i|$ . Since  $P_1, \dots, P_\ell$  are pair-wise commuting subgroups of  $G$ , the mapping

$$\iota : \Omega_1 \times \cdots \times \Omega_\ell \rightarrow \Omega$$

defined by  $(\omega^{g_1}, \dots, \omega^{g_\ell}) \mapsto \omega^{g_1 \cdots g_\ell}$  (with  $g_i \in P_i$ , for each  $i$ ) is well-defined and injective. Thus  $\iota$  is bijective. Now,  $\iota$  determines a permutation isomorphism between the natural product action of  $G$  on  $\Omega_1 \times \cdots \times \Omega_\ell$  and the action of  $G$  on  $\Omega$ .  $\square$

*Proof of Theorem 1.2.* For each  $i \in \{1, \dots, \ell\}$ , let  $P_i$  be a nilpotent transitive group of degree  $p_i^{\alpha_i}$  and nilpotency class at most  $c$  with  $|P_i| = F_{\text{Nil}}(p_i^{\alpha_i}, c)$ . Then  $G := P_1 \times \cdots \times P_\ell$ , endowed with its natural product action, is transitive of degree  $\prod_{i=1}^\ell p_i^{\alpha_i} = n$ , has nilpotency class at most  $c$ , and  $|G| = \prod_{i=1}^\ell F_{\text{Nil}}(p_i^{\alpha_i}, c)$ . Thus  $\prod_{i=1}^\ell F_{\text{Nil}}(p_i^{\alpha_i}, c) \leq F_{\text{Nil}}(n, c)$ .

Conversely, let  $G$  be a nilpotent transitive group of degree  $n$  and nilpotency class at most  $c$  with  $|G| = F_{\text{Nil}}(n, c)$ . By Proposition 2.1,  $G = P_1 \times \cdots \times P_\ell$ ,  $P_i$  is the Sylow  $p_i$ -subgroup of  $G$ , and  $P_i$  has a faithful transitive action of degree  $p_i^{\alpha_i}$ . Thus  $F_{\text{Nil}}(n, c) = |G| = \prod_{i=1}^\ell |P_i| \leq \prod_{i=1}^\ell F_{\text{Nil}}(p_i^{\alpha_i}, c)$ .  $\square$

The following two facts hardly deserve to be called lemmas, but will be used several times.

**Lemma 2.2.** *Let  $K$  be a transitive permutation group on  $\Omega$ . If  $K$  centralises  $g \in \text{Sym}(\Omega)$  and  $g$  fixes some point of  $\Omega$ , then  $g = 1$ .*

*Proof.* Let  $\omega$  be an element of  $\Omega$  fixed by  $g$ . For every  $k \in K$ , we have  $(\omega^k)^g = \omega^{kg} = \omega^{gk} = \omega^k$  and hence  $g$  fixes  $\omega^k$ . Since  $K$  is transitive,  $g$  fixes every element of  $\Omega$  and hence  $g = 1$ .  $\square$

**Lemma 2.3.** *Let  $k$  and  $\ell$  be positive integers, let  $K$  be a group and let  $H_1, \dots, H_\ell$  be subgroups of  $K$  with  $|K : H_i| = k$ , for each  $i$ . Then  $|K : \cap_{i=1}^\ell H_i| \leq k^\ell$ .*

*Proof.* Note that if  $A$  and  $B$  are subgroups of  $K$ , then  $|K : A \cap B| \leq |K : A| |K : B|$ . Now, the proof follows by induction on  $\ell$ .  $\square$

Now we prove an elementary upper bound for  $F_{\text{Nil}}(p^k, c)$ . This upper bound is weaker than the upper bound in Theorem 1.5. However, its proof is elementary and contains the main ingredients (but not the technicalities) of the proof of Theorem 1.5. In particular, we hope this makes the flow of the argument in Theorem 1.5 easier to follow.

**Proposition 2.4.** *Let  $k$  and  $c$  be positive integers and let  $p$  be a prime number. Then  $\log_p(F_{\text{Nil}}(p^k, c)) \leq k(k^c - 1)/(k - 1)$ .*

*Proof.* Let  $G$  be a nilpotent transitive permutation group of degree  $p^k$  and nilpotency class at most  $c$ , let  $\Omega$  be the set acted upon by  $G$ , let  $\omega \in \Omega$  and let  $H$  be the point stabiliser  $G_\omega$ . Observe that  $\gamma_c(G) \leq \mathbf{Z}(G)$  and hence  $\gamma_c(G) \cap H = 1$  by Lemma 2.2. We show that  $\log_p(|G|) \leq k(k^c - 1)/(k - 1)$ , from which the proof follows from the definition of  $F_{\text{Nil}}(p^k, c)$ .

Set  $g_0 := 1$  and  $K_0 := \langle g_0 \rangle$ . For  $i > 0$ , we define recursively  $g_i$  and  $K_i$ . If  $K_{i-1}H$  is a proper subset of  $G$ , then choose  $g_i \in G \setminus K_{i-1}H$  and set  $K_i := \langle K_{i-1}, g_i \rangle$ . If  $G = K_{i-1}H$ , then choose  $g_i := 1$  and  $K_i := \langle K_{i-1}, g_i \rangle = K_{i-1}$ . Let  $\ell$  be the minimum positive integer with  $K_\ell = K_{\ell+1}$ . By construction,  $G = K_\ell H$  and hence  $K_\ell$  is transitive on  $\Omega$ . Moreover, since  $|G : H| = |\Omega| = p^k$  and  $|K_i H| < |K_{i+1} H|$  for each  $i \in \{0, \dots, \ell - 1\}$ , we have  $\ell \leq k$ .

For  $\kappa \in \{1, \dots, c - 1\}$ , define

$$L_\kappa := \bigcap_{i_1, \dots, i_{c-\kappa}=0}^\ell (\gamma_\kappa(G) \cap H)^{g_{i_1} \cdots g_{i_{c-\kappa}}}.$$

By taking  $i_1 = \dots = i_{c-\kappa} = 0$  we see that  $\gamma_\kappa(G) \cap H$  is one of the terms of this intersection, and hence  $L_\kappa \leq \gamma_\kappa(G) \cap H$ .

We claim that  $L_\kappa = 1$ . We argue inductively on  $c - \kappa$ . If  $c - \kappa = 1$ , then  $\kappa = c - 1$  and  $L_{c-1} = \bigcap_{i=0}^\ell (\gamma_{c-1}(G) \cap H)^{g_i}$ . Let  $y$  be in  $L_{c-1}$ . As  $y \in (\gamma_{c-1}(G) \cap H)^{g_i}$ , there exists  $h_i \in \gamma_{c-1}(G) \cap H$  with  $y = h_i^{g_i}$ . Since  $h_i$  and  $y$  are both in  $H$ , we have  $h_i^{-1}y = [h_i, g_i] \in \gamma_c(G) \cap H = 1$ , and hence  $h_i = y$ . It follows that  $y = h_i^{g_i} = y^{g_i}$  and hence  $y$  is centralised by  $g_i$ . Therefore  $y$  is centralised by  $\langle g_0, \dots, g_\ell \rangle = K_\ell$ . Since  $K_\ell$  is transitive, by Lemma 2.2, we obtain  $y = 1$ , and the base case of the induction is proved.

Now suppose that  $c - \kappa > 1$ . Let  $y$  be in  $L_\kappa$ . Fix  $i_1, \dots, i_{c-\kappa} \in \{0, \dots, \ell\}$ . As  $y \in (\gamma_\kappa(G) \cap H)^{g_{i_1} \cdots g_{i_{c-\kappa}}}$ , there exists  $h_{i_1, \dots, i_{c-\kappa}} \in \gamma_\kappa(G) \cap H$  with

$$y = (h_{i_1, \dots, i_{c-\kappa}})^{g_{i_1} \cdots g_{i_{c-\kappa}}}.$$

Thus  $(h_{i_1, \dots, i_{c-\kappa}})^{-1}y = [h_{i_1, \dots, i_{c-\kappa}}, g_{i_1} \cdots g_{i_{c-\kappa}}]$ . As both  $y$  and  $h_{i_1, \dots, i_{c-\kappa}}$  are in  $H$ , we may write  $h_{i_1, \dots, i_{c-\kappa}} = yz_{i_1, \dots, i_{c-\kappa}}$ , where  $z_{i_1, \dots, i_{c-\kappa}} = [h_{i_1, \dots, i_{c-\kappa}}, g_{i_1} \cdots g_{i_{c-\kappa}}]^{-1} \in \gamma_{\kappa+1}(G) \cap H$ . We obtain

$$(1) \quad y = (yz_{i_1, \dots, i_{c-\kappa}})^{g_{i_1} \cdots g_{i_{c-\kappa}}}.$$

Applying Eq. (1) with  $i_{c-\kappa} = 0$  and recalling that  $g_0 = 1$ , we have

$$(2) \quad y^{g_{i_1} \cdots g_{i_{c-(\kappa+1)}}} = y((z_{i_1, \dots, i_{c-(\kappa+1)}, 0})^{-1})^{g_{i_1} \cdots g_{i_{c-(\kappa+1)}}}.$$

Eq. (1) (applied twice, first to the  $(c - \kappa)$ -tuple  $0, \dots, 0, i_{c-\kappa}$  and then to the  $(c - \kappa)$ -tuple  $i_1, \dots, i_{c-\kappa}$ ) gives

$$\begin{aligned} (yz_{0, \dots, 0, i_{c-\kappa}})^{g_{i_{c-\kappa}}} &= y = (yz_{i_1, \dots, i_{c-\kappa}})^{g_{i_1} \cdots g_{i_{c-\kappa}}} \\ &= ((yz_{i_1, \dots, i_{c-\kappa}})^{g_{i_1} \cdots g_{i_{c-(\kappa+1)}}})^{g_{i_{c-\kappa}}} \end{aligned}$$

and hence

$$yz_{0,\dots,0,i_{c-\kappa}} = (yz_{i_1,\dots,i_{c-\kappa}})^{g_{i_1}\cdots g_{i_{c-(\kappa+1)}}} = y^{g_{i_1}\cdots g_{i_{c-(\kappa+1)}}} (z_{i_1,\dots,i_{c-\kappa}})^{g_{i_1}\cdots g_{i_{c-(\kappa+1)}}}.$$

From this and Eq. (2), we obtain

$$(3) \quad z_{0,\dots,0,i_{c-\kappa}} = ((z_{i_1,\dots,i_{c-(\kappa+1)},0})^{-1} z_{i_1,\dots,i_{c-\kappa}})^{g_{i_1}\cdots g_{i_{c-(\kappa+1)}}}.$$

In particular,  $z_{0,\dots,0,i_{c-\kappa}} \in (\gamma_{\kappa+1}(G) \cap H)^{g_{i_1}g_{i_2}\cdots g_{i_{c-(\kappa+1)}}}$ . As  $i_1, \dots, i_{c-\kappa}$  is an arbitrary  $(c-\kappa)$ -tuple of elements of  $\{0, \dots, \ell\}$ , Eq. (3) gives

$$z_{0,\dots,0,i_{c-\kappa}} \in \bigcap_{i_1,\dots,i_{c-(\kappa+1)}=0}^{\ell} (\gamma_{\kappa+1}(G) \cap H)^{g_{i_1}g_{i_2}\cdots g_{i_{c-(\kappa+1)}}} = L_{\kappa+1} = 1,$$

where in the last equality we used the inductive hypothesis. Thus  $z_{0,\dots,0,i_{c-\kappa}} = 1$ .

Applying Eq. (1) with  $i_1 = \dots = i_{c-(\kappa+1)} = 0$ , we deduce  $y = y^{g_{i_{c-\kappa}}}$ . Therefore  $y$  is centralised by  $\langle g_0, \dots, g_{\ell} \rangle = K_{\ell}$ . Now Lemma 2.2 yields  $y = 1$ . As  $y$  is an arbitrary element of  $L_{\kappa}$ , we get  $L_{\kappa} = 1$ , and this concludes the proof of our claim.

For  $\kappa = 1$ , we have

$$(4) \quad L_1 = \bigcap_{i_1,\dots,i_{c-1}=0}^{\ell} H^{g_{i_1}\cdots g_{i_{c-1}}} = 1.$$

Observe that in the intersection in (4) there are exactly  $1 + \ell + \dots + \ell^{c-1} = (\ell^c - 1)/(\ell - 1)$  terms: 1 accounts for the term of the intersection with  $i_1 = \dots = i_{c-1} = 0$ ,  $\ell$  accounts for the terms of the intersection with exactly one  $i_j \neq 0$ , etc. In particular,  $L_1$  is the intersection of  $(\ell^c - 1)/(\ell - 1)$  subgroups of  $G$  having index  $p^k$ . Therefore, by Lemma 2.3,

$$|G| = |G : L_1| \leq (p^k)^{(\ell^c - 1)/(\ell - 1)}.$$

As  $\ell \leq k$ , the proposition is proved.  $\square$

When  $c = 1$ , Proposition 2.4 gives  $F_{\text{Nil}}(p^k, 1) \leq p^k$ , and hence this upper bound equals  $F_{\text{Nil}}(p^k, 1)$ . However, for larger values of  $c$ , the upper bound in Proposition 2.4 is far from optimal. For instance, when  $c = 2$ , Proposition 2.4 gives  $F_{\text{Nil}}(p^k, 2) \leq p^{k+k^2}$ , but in fact Theorem 1.3 shows that  $F_{\text{Nil}}(p^k, 2) = p^{k+\lfloor k/2 \rfloor \lceil k/2 \rceil}$ .

We conclude this preliminary section making an observation on the minimal order  $f_{\text{Nil}}(p^k, c)$  of a nilpotent transitive group of degree  $p^k$  and nilpotency class  $c$ .

**Remark 2.5.** Suppose that  $c \leq k - 1$ . Let  $P$  be a group of order  $p^{c+1}$  and maximal class, that is,  $P$  has nilpotency class  $c$ . Let  $Q$  be an abelian group of order  $p^{k-c-1}$  and set  $G := P \times Q$ . Then  $G$  has nilpotency class  $c$  and, via its right regular representation, is transitive of degree  $p^k$ . Therefore  $f_{\text{Nil}}(p^k, c) = p^k$ . This suggests that the function  $f_{\text{Nil}}(p^k, c)$  becomes interesting only when  $c$  is large compared to  $k$ .

We make another example along these lines. This example is inspired by [4, Section 3, Exercise 3.4] (see also [1, Proposition 9.15]). Suppose that  $c \leq (k - 1)(p - 1)$  and write  $c = q(p - 1) + r$  with  $0 \leq r < p - 1$ . Observe that  $q < k - 1$  if  $r > 0$ , and  $q \leq k - 1$  if  $r = 0$ . From [4, Exercise 3.4], there exists a  $p$ -group  $P$  of maximal class  $c$  with  $P = M \rtimes \langle x \rangle$  such that

- (i)  $x$  has order  $p$ ,
- (ii)  $M = \langle x_1 \rangle \times \langle x_2 \rangle \times \dots \times \langle x_{p-1} \rangle$  is abelian,
- (iii)  $|x_1| = \dots = |x_r| = p^{q+1}$  and  $|x_{r+1}| = \dots = |x_{p-1}| = p^q$ ,

(iv)  $\mathbf{Z}(P) = \langle x_r^{p^q} \rangle$  if  $r > 0$ , and  $\mathbf{Z}(P) = \langle x_{p-1}^{p^{q-1}} \rangle$  if  $r = 0$ .

Set  $H := \langle x_1, \dots, x_{r-1}, x_{r+1}, \dots, x_{p-1} \rangle$  if  $r > 0$ , and  $H := \langle x_1, \dots, x_{p-2} \rangle$  if  $r = 0$ . Now,  $H \cap \mathbf{Z}(P) = 1$  and hence  $H$  is core-free in  $P$ . Let  $\Delta$  be the set of right cosets of  $H$  in  $P$ . Clearly,  $|\Delta| = |P : H| = p^{q+2}$  if  $r > 0$ , and  $|\Delta| = p^{q+1}$  if  $r = 0$ . Let  $Q$  be an abelian group of order  $p^{k-q-2}$  if  $r > 0$ , and order  $p^{k-q-1}$  if  $r = 0$ . Set  $G := P \times Q$  and  $\Omega := \Delta \times Q$ . Then  $G$  has nilpotency class  $c$  and, via its natural product action, is transitive and faithful on  $\Omega$  of degree  $p^k$ . Now,  $|G| = p^{k+q(p-2)+r-1}$  if  $r > 0$ , and  $|G| = p^{k+q(p-2)}$  if  $r = 0$ . As  $q = (c-r)/(p-1)$ , in both cases we obtain  $|G| \leq p^{k+c(p-2)/(p-1)}$ . Therefore

$$p^k \leq f_{\text{Nil}}(p^k, c) \leq p^{k+c(p-2)/(p-1)} < p^{k+c}.$$

### 3. NILPOTENCY CLASS 2

Before moving to transitive  $p$ -groups of arbitrary nilpotency class  $c$ , we start a detailed discussion of the transitive  $p$ -groups of nilpotency class 2. First, this has the benefit of highlighting the type of improvements that are needed in Proposition 2.4 to obtain Theorem 1.5. Second, when  $c = 2$ , we give an explicit formula for  $F_{\text{Nil}}(p^k, 2)$  and we describe the transitive  $p$ -groups  $G$  of nilpotency class 2 with  $|G| = F_{\text{Nil}}(p^k, 2)$ , which gives a complete understanding of the case  $c \leq 2$ .

We start with an elementary example, which will hopefully help to follow the more general construction in Example 3.2 and the proof of Theorem 1.3.

**Example 3.1.** Let  $p$  be a prime, let  $k$  be a positive integer and let  $m \in \{\lfloor k/2 \rfloor, \lceil k/2 \rceil\}$ . Let  $V = \langle e_1, \dots, e_k \rangle$  be the  $k$ -dimensional vector space of row vectors over the field  $\mathbb{F}_p$  of size  $p$ , and let  $H$  be the group of (block) unitriangular matrices

$$H = \left\{ \begin{pmatrix} I_m & 0 \\ A & I_{k-m} \end{pmatrix} \mid A \text{ is an } (k-m) \times m\text{-matrix with coefficients in } \mathbb{F}_p \right\}$$

where, for a positive integer  $\ell$ ,  $I_\ell$  denotes the  $\ell \times \ell$ -identity matrix with coefficients in  $\mathbb{F}_p$ . Let  $G$  be the affine group of linear transformations  $H \ltimes V$ . The group  $G$  acts faithfully and transitively on the underlying set  $V$ , with  $V$  acting by translations and with  $H$  acting by matrix multiplication, that is,  $v^{(h,w)} := vh + w$ , for each  $v \in V$  and  $(h, w) \in H \ltimes V$ .

A computation shows that, for  $k > 1$ ,  $\mathbf{Z}(G) = \langle e_1, \dots, e_m \rangle = \gamma_2(G)$  and hence  $G$  has nilpotency class 2. Clearly  $\log_p(|G|) = \log_p(|H||V|) = k + m(k-m) = k + \lfloor k/2 \rfloor \lceil k/2 \rceil$ .

In the next example we generalise the construction in Example 3.1.

**Example 3.2.** Let  $p$  be a prime, let  $k$  be a positive integer, let  $m \in \{\lfloor k/2 \rfloor, \lceil k/2 \rceil\}$ , let  $V$  be an abelian group of order  $p^k$  and let  $Z$  be a subgroup of  $V$ . Suppose that  $|Z| = p^m$  and that both  $V/Z$  and  $Z$  are elementary abelian. Let  $v_1, \dots, v_{k-m}$  be generators of  $V$  modulo  $Z$ , let  $W := \langle v_1^p, \dots, v_{k-m}^p \rangle$  and let  $Z'$  be a complement of  $W$  in  $Z$ . Write  $p^a := |W|$ , for some  $a \in \{0, \dots, m\}$ . Let  $w_1, \dots, w_{m-a}$  be generators of  $Z'$ .

Since the Frattini subgroup of  $V$  is  $W$ , we see that  $V$  is generated by

$$S := \{v_1, \dots, v_{k-m}, w_1, \dots, w_{m-a}\}.$$

For every  $z_1, \dots, z_{k-m} \in Z$ , let  $\varphi_{z_1, \dots, z_{k-m}}$  be the automorphism of  $V$  defined on the generating set  $S$  by

$$\begin{aligned} v_i^{\varphi_{z_1, \dots, z_{k-m}}} &:= v_i z_i, & \text{for every } i \in \{1, \dots, k-m\}, \\ w_j^{\varphi_{z_1, \dots, z_{k-m}}} &:= w_j, & \text{for every } j \in \{1, \dots, m-a\}, \end{aligned}$$

and let  $H$  be the subgroup of  $\text{Aut}(V)$  generated by all such functions. Clearly,  $H$  is an elementary abelian  $p$ -group of order  $|Z|^{k-m} = p^{m(k-m)}$ .

Let  $G$  be the semidirect product  $V \rtimes H$ . As in Example 3.1, the group  $G$  acts faithfully and transitively on the underlying set  $V$ , with  $V$  acting by right multiplications and with  $H$  acting by conjugation.

A computation shows that, for  $k > 1$ ,  $\mathbf{Z}(G) = Z = \gamma_2(G)$  and hence  $G$  has nilpotency class 2. Clearly  $\log_p(|G|) = k + \lfloor k/2 \rfloor \lceil k/2 \rceil$ .

**Remark 3.3.** A tedious computation and the structure theorem of finite abelian groups show that, for  $p$  odd, there are  $k+1$  pair-wise permutation non-isomorphic groups in Example 3.2 when  $k > 1$  is odd, and  $k/2 + 1$  when  $k$  is even.

The situation when  $p = 2$  is remarkably different. Indeed, every group in Example 3.2 is permutation isomorphic to one of the groups in Example 3.1.

*Proof of Theorem 1.3.* Let  $G$  be a nilpotent transitive group of degree  $p^k$  and nilpotency class at most 2. Write  $Z := \mathbf{Z}(G)$  and let  $H$  be the stabiliser in  $G$  of a point. As  $H$  is core-free in  $G$ , we get  $H \cap Z = 1$  and hence  $HZ/Z \cong H$ . As  $G/Z$  is abelian, we obtain that  $H$  is abelian and  $\langle H, Z \rangle = HZ = H \times Z$ . Since  $G$  has nilpotency class at most 2, every subgroup of  $G$  containing  $Z$  is normal, and hence  $HZ \trianglelefteq G$ .

Write  $p^a := |Z|$ . Thus  $|G : HZ| = p^{k-a}$ . Let  $b$  be the minimum positive integer such that there exist  $g_1, \dots, g_b \in G$  with  $G = \langle g_1, \dots, g_b, HZ \rangle$ . Observe that  $b \leq k - a$ . We claim that

$$H \cap \bigcap_{i=1}^b H^{g_i} = 1.$$

Write  $Y := H \cap \bigcap_{i=1}^b H^{g_i}$  and take  $y \in Y$ . For every  $i \in \{1, \dots, b\}$ , we have  $y \in H^{g_i}$  and hence  $y = h_i^{g_i}$ , for some  $h_i \in H$ . Therefore  $y = h_1^{g_1} = \dots = h_b^{g_b}$ . Observe that  $h_i^{g_i} = h_i[h_i, g_i] \in H \times Z$  and, since  $y \in H$ , we get  $y = h_i$  and  $[h_i, g_i] = 1$ . In particular,  $y$  is centralised by  $g_1, \dots, g_b$ . As  $y \in H$  and  $H$  is abelian,  $y$  is centralised by  $H$  and hence by  $\langle g_1, \dots, g_b, HZ \rangle = G$ . Thus  $y \in \mathbf{Z}(G) = Z$  and hence  $y = 1$ .

As  $HZ \trianglelefteq G$ , we see that  $H, H^{g_1}, \dots, H^{g_b}$  are  $b+1$  subgroups of  $HZ$  of index  $p^a$ . As  $H \cap \bigcap_{i=1}^b H^{g_i} = 1$ , we get  $|HZ| \leq (p^a)^{b+1}$  from Lemma 2.3. Thus

$$(5) \quad |G| = |G : HZ| |HZ| \leq p^{k-a} \cdot p^{a(b+1)} \leq p^{k-a+a(k-a+1)} = p^{k+a(k-a)}.$$

The maximum of the function  $a \mapsto a(k-a)$  is attained at  $a \in \{\lfloor k/2 \rfloor, \lceil k/2 \rceil\}$ . Therefore  $|G| \leq p^{k+\lfloor k/2 \rfloor \lceil k/2 \rceil}$  and hence  $F_{\text{Nil}}(p^k, 2) \leq p^{k+\lfloor k/2 \rfloor \lceil k/2 \rceil}$ . The groups in Example 3.1 have order  $p^{k+\lfloor k/2 \rfloor \lceil k/2 \rceil}$ , are transitive of degree  $p^k$  and have nilpotency class at most 2. Thus  $p^{k+\lfloor k/2 \rfloor \lceil k/2 \rceil} \leq F_{\text{Nilp}}(p^k, 2)$ . This concludes the proof of the first assertion.

Let  $G$  be a transitive group of degree  $p^k$ , of nilpotency class at most 2 and with  $|G| = F_{\text{Nil}}(p^k, 2)$ . From Eq. (5), we have  $a \in \{\lfloor k/2 \rfloor, \lceil k/2 \rceil\}$  and  $b = k - a$ . Hence the minimum number of generators of  $G/HZ$  is  $k - a$  and thus  $G/HZ$  is elementary



abelian. Again from Eq. (5) we deduce  $|H| = p^{a(k-a)}$ . Since  $H \cap \bigcap_{i=1}^{k-a} H^{g_i} = 1$ , with an inductive argument we obtain

$$(6) \quad |H : H \cap \bigcap_{i \in I} H^{g_i}| = p^{a|I|},$$

for every subset  $I$  of  $\{1, \dots, k-a\}$ .

When  $k = 1$ ,  $G$  is cyclic of order  $p$  and  $G$  is one of the groups in Example 3.2. Therefore, for the rest of this proof we assume  $k > 1$ .

For each  $i \in \{1, \dots, k-a\}$ , define

$$(7) \quad C_i := H \cap \bigcap_{\substack{j=1 \\ j \neq i}}^{k-a} H^{g_j}.$$

Since  $|H| = p^{a(k-a)}$ , from Eq. (6) we obtain  $|C_i| = p^a$ . Moreover, as  $|H : H \cap H^{g_i}| = p^a$  and  $C_i \cap H^{g_i} = 1$ , we get

$$(8) \quad H = C_i(H \cap H^{g_i}).$$

Since  $|HZ : H^{g_i}| = |H : H \cap H^{g_i}|$ , we deduce  $HZ = HH^{g_i}$  and, as  $HH^{g_i} = H[H, g_i]$ , we get  $HZ = H[H, g_i]$ . Now,  $[H, g_i] \leq Z$  and hence

$$Z = [H, g_i].$$

It follows that the mapping  $[-, g_i] : H \rightarrow Z$  defined by  $h \mapsto [h, g_i]$  is surjective. Thus  $\mathbf{C}_H(g_i) = \ker([-, g_i]) \leq H$  and  $|H : \mathbf{C}_H(g_i)| = |Z| = p^a$ . Since  $\mathbf{C}_H(g_i) \leq H \cap H^{g_i}$ , we obtain

$$(9) \quad \mathbf{C}_H(g_i) = H \cap H^{g_i}$$

and  $\bigcap_{j=1}^{k-a} \mathbf{C}_H(g_j) = 1$ . Thus  $H$  is a subdirect subgroup of the direct product of  $k-a$  copies of  $Z$ . Since  $|H| = |Z|^{k-a}$ , we get  $H \cong Z^{k-a}$  and  $H$  is abelian.

From Eqs. (7) and (9), we get  $C_i = \bigcap_{j \neq i} \mathbf{C}_H(g_j)$ . From Eq. (8), it follows that

$$Z = [H, g_i] = [C_i(H \cap H^{g_i}), g_i] = [C_i \mathbf{C}_H(g_i), g_i] = [C_i, g_i].$$

Since  $g_i$  has order  $p$  modulo  $HZ$  and since  $G$  has nilpotency class at most 2, we have  $1 = [h, g_i^p] = [h, g_i]^p$  for every  $h \in H$ , which gives that  $[H, g_i] = Z$  has exponent  $p$ . As  $H \cong Z^{k-a}$ ,  $H$  has also exponent  $p$ .

Next we show that there exist  $h_1, \dots, h_{k-a} \in H$  with  $\langle g_1 h_1, \dots, g_{k-a} h_{k-a} \rangle$  abelian. Let  $i$  be an element of  $\{1, \dots, k-a\}$ . For  $j \in \{i+1, \dots, k-a\}$ , let  $z_j \in C_j$  with  $[g_i, g_j] = [z_j, g_j]^{-1}$  (observe that  $[g_i, g_j] \in \gamma_2(G) \leq Z = [C_j, g_j]$  and hence there exists such an element  $z_j$ ). Define  $h_i := \prod_{j=i+1}^{k-a} z_j$ . Observe that, for every  $r \in \{1, \dots, k-a\}$ , the element  $g_r$  commutes with  $C_1, \dots, C_{r-1}, C_{r+1}, \dots, C_{k-a}$  and hence  $g_r$  commutes with  $z_s$ , for every  $s \in \{1, \dots, k-a\}$  with  $r \neq s$ . Now, let  $i, j \in \{1, \dots, k-a\}$  with  $i < j$ . Since  $G$  has nilpotency class at most 2 and  $H$  is abelian, we have

$$\begin{aligned} [g_i h_i, g_j h_j] &= [g_i, g_j][g_i, h_j][h_i, g_j] = [z_j, g_j]^{-1} \prod_{\ell=j+1}^{k-a} [g_i, z_\ell] \prod_{\ell=i+1}^{k-a} [z_\ell, g_j] \\ &= [z_j, g_j]^{-1} [z_j, g_j] = 1. \end{aligned}$$

Write  $V := \langle g_1 h_1, \dots, g_{k-a} h_{k-a}, Z \rangle$ . Since  $Z \leq V$ , we have  $V \trianglelefteq G$ . As  $\langle g_1 h_1, \dots, g_{k-a} h_{k-a} \rangle$  is abelian, so is  $V$ . By construction  $V$  is transitive and hence  $V \cap H = 1$ . This gives  $|V| = p^k$  and  $G$  is isomorphic to the semidirect product

$V \rtimes H$ . As  $G/HZ$  is elementary abelian, so is  $V/Z$ . Thus  $V/Z$  and  $Z$  are both elementary abelian. Finally, observe that  $H$  centralises every element of  $V/Z$  and  $Z$ . In particular,  $G$  is permutation isomorphic to one of the groups in Example 3.2.  $\square$

**Remark 3.4.** Let  $N$  denote the number (up to permutation isomorphism) of nilpotent transitive groups of degree  $p^k$ , nilpotency class 2 and order  $F_{\text{Nil}}(p^k, 2)$ . Theorem 1.3 and Remark 3.3 show that

$$N = \begin{cases} 0 & \text{when } k = 1, \\ 1 & \text{when } p = 2 \text{ and } k \text{ is even,} \\ 2 & \text{when } p = 2 \text{ and } k > 1 \text{ is odd,} \\ k/2 + 1 & \text{when } p > 2 \text{ and } k \text{ is even,} \\ k + 1 & \text{when } p > 2 \text{ and } k > 1 \text{ is odd.} \end{cases}$$

#### 4. PROOF OF THEOREM 1.5

*Proof of Theorem 1.5.* Let  $G$  be a nilpotent transitive permutation group of degree  $p^k$  and nilpotency class at most  $c$ , let  $\Omega$  be the set acted upon by  $G$ , let  $\omega \in \Omega$  and let  $H := G_\omega$ .

For  $i \in \{1, \dots, c\}$ , define  $a_i := \log_p(|\gamma_i(G)H : \gamma_{i+1}(G)H|)$ . Observe that  $|\gamma_c(G)H : \gamma_{c+1}(G)H| = |\gamma_c(G)H : H| = |\gamma_c(G) : \gamma_c(G) \cap H| = |\gamma_c(G)|$  by Lemma 2.2, and hence  $a_c = \log_p(|\gamma_c(G)|)$ . Moreover,  $k = \log_p(|G : H|) = \sum_{i=1}^c \log_p(|\gamma_i(G)H : \gamma_{i+1}(G)H|) = \sum_{i=1}^c a_i$ .

We show, by induction on  $c$ , that

$$(10) \quad \log_p(|G|) \leq \sum_{i=1}^c a_i \left( \frac{\left( \sum_{j=1}^{i-1} a_j \right)^i - 1}{\left( \sum_{j=1}^{i-1} a_j \right) - 1} \right).$$

Denote by  $T(a_1, \dots, a_c)$  the right-hand side of Eq. (10). When  $c = 1$ , the group  $G$  is abelian; thus  $a_1 = k$  and  $\log_p(|G|) = k = T(a_1)$ .

Suppose that  $c > 1$ . Let  $U$  be the core of  $\gamma_c(G)H$  in  $G$ , that is,

$$U := \bigcap_{g \in G} (\gamma_c(G)H)^g.$$

As  $\gamma_c(G) \leq U$ , we have  $\gamma_c(G)H \leq UH$ . Moreover, since  $U \leq \gamma_c(G)H$ , we also have  $UH \leq \gamma_c(G)H$ . Thus  $UH = \gamma_c(G)H$ .

We write  $\bar{G} := G/U$  and we adopt the “bar” notation: for a subgroup  $X$  of  $G$ ,  $\bar{X}$  denotes  $XU/U$ .

Let  $\mathcal{B}$  be the set of orbits of  $\gamma_c(G)$  on  $\Omega$ . Observe that  $\mathcal{B}$  is a  $G$ -set, that is, the action of  $G$  on  $\Omega$  induces an action of  $G$  on  $\mathcal{B}$  by setting  $(\delta^{\gamma_c(G)})^g = (\delta^g)^{\gamma_c(G)}$ , for every  $\delta \in \Omega$  and  $g \in G$ .

For  $\delta \in \Omega$ , we have  $|\delta^{\gamma_c(G)}| = |\gamma_c(G) : \gamma_c(G) \cap G_\delta| = |\gamma_c(G)| = p^{a_c}$  and hence  $|\mathcal{B}| = |\Omega|/p^{a_c} = p^{k-a_c}$ . Moreover, the setwise stabiliser of  $\omega^{\gamma_c(G)}$  is  $\gamma_c(G)H$  and hence the kernel of the action of  $G$  on  $\mathcal{B}$  is  $U$ . Therefore  $G/U = \bar{G}$  is a transitive permutation group of degree  $p^{k-a_c}$  on  $\mathcal{B}$  and the stabiliser in  $\bar{G}$  of the point  $\omega^{\gamma_c(G)}$  of  $\mathcal{B}$  is  $\gamma_c(G)H/U = UH/U = \bar{H}$ .

Since  $U$  fixes setwise every  $\gamma_c(G)$ -orbit, we have  $\omega^U \subseteq \omega^{\gamma_c(G)}$ . Moreover, as  $\gamma_c(G) \leq U$ , we get  $\omega^U = \omega^{\gamma_c(G)}$ . From the Frattini argument it follows that  $U = \gamma_c(G)(U \cap G_\omega) = \gamma_c(G)(U \cap H)$ .

As  $\gamma_c(G) \leq U$ , we see that  $G/U = \bar{G}$  has nilpotency class at most  $c - 1$ . For  $i \in \{1, \dots, c - 1\}$ , we have

$$\gamma_i(\bar{G})\bar{H} = \frac{\gamma_i(G)U}{U} \frac{UH}{U} = \frac{\gamma_i(G)\gamma_c(G)(U \cap H)H}{U} = \frac{\gamma_i(G)H}{U}.$$

It follows that

$$\log_p(|\gamma_i(\bar{G})\bar{H} : \gamma_{i+1}(\bar{G})\bar{H}|) = \log_p(|\gamma_i(G)H : \gamma_{i+1}(G)H|) = a_i.$$

In particular, applying our inductive hypothesis to the permutation group  $\bar{G}$  we obtain

$$(11) \quad \log_p(|\bar{G}|) \leq T(a_1, \dots, a_{c-1}).$$

Set  $g_0 := 1$  and  $K_0 := \langle g_0 \rangle$ . For  $i > 0$ , we define recursively  $g_i$  and  $K_i$ . If  $K_{i-1}\gamma_c(G)H$  is a proper subset of  $G$ , then choose  $g_i \in G \setminus K_{i-1}\gamma_c(G)H$  and set  $K_i := \langle K_{i-1}, g_i \rangle$ . If  $G = K_{i-1}\gamma_c(G)H$ , then choose  $g_i := 1$  and  $K_i := \langle K_{i-1}, g_i \rangle = K_{i-1}$ . Let  $\ell$  be the minimum positive integer with  $K_\ell = K_{\ell+1}$ . By construction,  $G = K_\ell\gamma_c(G)H$  and hence  $K_\ell$  is transitive on  $\mathcal{B}$ . Moreover, since  $|G : \gamma_c(G)H| = |\mathcal{B}| = p^{k-a_c}$  and  $|K_i\gamma_c(G)H| < |K_{i+1}\gamma_c(G)H|$  for each  $i \in \{0, \dots, \ell - 1\}$ , we have  $\ell \leq k - a_c$ .

For  $\kappa \in \{1, \dots, c - 1\}$ , define

$$L_\kappa := \bigcap_{i_1, \dots, i_{c-\kappa}=0}^{\ell} (\gamma_\kappa(G) \cap H \cap U)^{g_{i_1} \cdots g_{i_{c-\kappa}}}.$$

Following verbatim the proof of Proposition 2.4 and observing that  $\gamma_c(G) \leq \mathbf{Z}(G)$ , we get  $L_\kappa = 1$ . When  $\kappa = 1$ , we deduce that  $L_1 = 1$  is the intersection of  $(\ell^c - 1)/(\ell - 1)$  subgroups of  $U$  having index  $p^{a_c}$ . Therefore, as  $\ell \leq k - a_c$ , by Lemma 2.3 we get

$$(12) \quad \log_p(|U|) \leq a_c \frac{(k - a_c)^c - 1}{(k - a_c) - 1}.$$

Now, observe that

$$(13) \quad \begin{aligned} T(a_1, \dots, a_c) &= T(a_1, \dots, a_{c-1}) + a_c \left( \frac{\left( \sum_{j=1}^{c-1} a_j \right)^c - 1}{\left( \sum_{j=1}^{c-1} a_j \right) - 1} \right) \\ &= T(a_1, \dots, a_{c-1}) + a_c \frac{(k - a_c)^c - 1}{(k - a_c) - 1}. \end{aligned}$$

From this, Eqs. (11) and (12) yield  $\log_p(|G|) = \log_p(|\bar{G}|) + \log_p(|U|) \leq T(a_1, \dots, a_c)$  and Eq. (10) is proved. The definition of  $F_{\text{Nil}}(p^k, c)$  gives  $\log_p(F_{\text{Nil}}(p^k, c)) \leq T(a_1, \dots, a_c) \leq F(k, c)$ .  $\square$

**Proposition 4.1.** *Let  $p$  be a prime number and let  $c$  and  $k$  be positive integers. Then, when  $c$  is fixed,*

$$F(k, c) = \frac{(c - 1)^{c-1} k^c}{c^c} + o(k^{c-1}).$$

*Proof.* Let  $T(a_1, \dots, a_c)$  be  $\sum_{i=1}^c a_i \left( \frac{(\sum_{j=1}^{i-1} a_j)^{i-1}}{(\sum_{j=1}^{i-1} a_j)^{i-1} - 1} \right)$ , as in the proof of Theorem 1.5.

Consider  $T_i(a_1, \dots, a_c) := a_i \left( \frac{(\sum_{j=1}^{i-1} a_j)^{i-1}}{(\sum_{j=1}^{i-1} a_j)^{i-1} - 1} \right)$ , the  $i$ -th summand of  $T(a_1, \dots, a_c)$ .

We now prove that,

$$(14) \quad \max \left( T_i(a_1, \dots, a_c) \mid a_1, \dots, a_c \in \mathbb{N}, \sum_{j=1}^c a_j = k \right) \leq \sum_{j=1}^i \frac{(j-1)^{j-1} k^j}{j^j}.$$

In fact, since  $\sum_{j=1}^c a_j = k$ , we have that  $T_i(a_1, \dots, a_c) \leq a_i \left( \frac{(k-a_i)^{i-1}}{(k-a_i)^{i-1} - 1} \right)$  with  $0 \leq a_i \leq k$ . Observing that, when  $0 \leq a_i \leq k$ , the maximum value of  $a_i (k-a_i)^j$  is  $\frac{j^j k^{j+1}}{(j+1)^{j+1}}$  (attained in  $a_i = \frac{k}{j+1}$ ), we obtain that  $\frac{(k-a_i)^{i-1}}{(k-a_i)^{i-1} - 1} = \sum_{j=0}^{i-1} a_i (k-a_i)^j \leq \sum_{j=1}^i \frac{(j-1)^{j-1} k^j}{j^j}$ , and Eq. (14) follows.

Now, Eq. (14) implies that

$$\max \left( T_i(a_1, \dots, a_c) \mid a_1, \dots, a_c \in \mathbb{N}, \sum_{j=1}^c a_j = k \right) \leq \frac{(i-1)^{i-1} k^i}{i^i} + o(k^{i-1}),$$

from which we conclude

$$F(k, c) \leq \frac{(c-1)^{c-1} k^c}{c^c} + o(k^{c-1}).$$

On the other hand, for every  $a_1, \dots, a_c \in \mathbb{N}$  with  $\sum_{j=1}^c a_j = k$ , we have  $T(a_1, \dots, a_c) \geq T_c(a_1, \dots, a_c)$ . As  $T_c(a_1, \dots, a_c) = a_c \left( \frac{(k-a_c)^{c-1}}{(k-a_c)^{c-1} - 1} \right)$ , it follows that  $F(k, c) \geq \max \left( a_c \left( \frac{(k-a_c)^{c-1}}{(k-a_c)^{c-1} - 1} \right) \mid a_c \in \mathbb{N}, 0 \leq a_c \leq k \right)$ .

Now, for  $a_c \in \mathbb{N}$  and  $0 \leq a_c \leq k$ , the maximum of  $a_c \left( \frac{(k-a_c)^{c-1}}{(k-a_c)^{c-1} - 1} \right)$  is greater than or equal to  $\max \left( \frac{k}{c} \left( \frac{(k-\frac{k}{c})^{c-1}}{(k-\frac{k}{c})^{c-1} - 1} \right), \left( \frac{k}{c} + 1 \right) \left( \frac{(k-(\frac{k}{c}+1))^{c-1}}{(k-(\frac{k}{c}+1))^{c-1} - 1} \right) \right)$ . A computation shows that  $\max \left( \frac{k}{c} \left( \frac{(k-\frac{k}{c})^{c-1}}{(k-\frac{k}{c})^{c-1} - 1} \right), \left( \frac{k}{c} + 1 \right) \left( \frac{(k-(\frac{k}{c}+1))^{c-1}}{(k-(\frac{k}{c}+1))^{c-1} - 1} \right) \right) \geq \frac{(c-1)^{c-1} k^c}{c^c} + o(k^{c-1})$ . In particular, we conclude that

$$F(k, c) \geq \frac{(c-1)^{c-1} k^c}{c^c} + o(k^{c-1})$$

and the proposition follows.  $\square$

Next we show that, for  $c$  small compared to  $k$ , the upper bound in Theorem 1.5 is closed to be optimal. The second author will always be in debt with Laci Kovács for pointing out and discussing [5] in 2005: in fact, the results in [5] have already played a role in the study of transitive  $p$ -groups, see for example [8, Section 3].

**Proposition 4.2.** *Let  $p$  be a prime number and let  $c$  and  $k$  be positive integers with  $c \mid k$ . Then,*

$$\log_p(F_{\text{Nil}}(p^k, c)) \geq \frac{k}{c} \binom{k(c-1)/c}{c-1}.$$

In particular, if  $c = o(k)$ , then

$$\log_p(F_{\text{Nil}}(p^k, c)) \geq \frac{(c-1)^{c-1}}{c^c(c-1)!} k^c + o(k^{c-1}).$$

*Proof.* Let  $u$  and  $v$  be positive integers. Let  $U$  be the Galois field  $\mathbb{F}_{p^u}$  of size  $p^u$  and let  $V$  be an  $\mathbb{F}_p$ -vector space of dimension  $v$  (over the field  $\mathbb{F}_p$  of size  $p$ ) with basis  $e_1, \dots, e_v$  and dual basis  $e_1^*, \dots, e_v^*$ .

Let  $W := U \wr V$  be the wreath product of  $U$  with  $V$ . Observe that by considering  $U$  and  $V$  as transitive regular permutation groups,  $W$  is transitive of degree  $|U||V| = p^{u+v}$  in its natural imprimitive action. Let  $B := U^V$  be the base group of  $W$ , that is,  $B$  consists of all functions from  $V$  to  $U$  and  $W = B \rtimes V$ .

Let  $\mathcal{S}$  be the symmetric  $U$ -algebra on  $e_1^*, \dots, e_v^*$  with natural grading

$$\mathcal{S} = \bigoplus_{m \in \mathbb{N}} \mathcal{S}_m,$$

where  $\mathcal{S}_m$  is spanned over  $U$  by the monomials  $e_{i_1}^{*j_1} \otimes \dots \otimes e_{i_\ell}^{*j_\ell}$  of degree  $m$ , that is,  $j_1 + \dots + j_\ell = m$ . Let  $\mathcal{M}_m$  be the  $U$ -subspace of  $\mathcal{S}_m$  spanned by the monomials  $e_{i_1}^{*j_1} \otimes \dots \otimes e_{i_\ell}^{*j_\ell}$  of degree  $m$  with  $j_r \leq p-1$ , for every  $r \in \{1, \dots, \ell\}$ .

Let  $\pi : \mathcal{S} \rightarrow B$  be the valuation map defined on the basis elements of  $\mathcal{S}$  by

$$\pi(e_{i_1}^{*j_1} \otimes \dots \otimes e_{i_\ell}^{*j_\ell})(x) := (e_{i_1}^*(x))^{j_1} \dots (e_{i_\ell}^*(x))^{j_\ell}.$$

Set  $Z_m := \pi(\mathcal{M}_m)$ .

From [5], we deduce that  $W$  has nilpotency class  $v(p-1) + 1$ ,  $\mathbf{Z}_m(W) = \gamma_{v(p-1)+2-m}(W)$  and  $B \cap \mathbf{Z}_m(W) = \bigoplus_{0 \leq i \leq m-1} Z_i$ . Moreover,  $\pi|_{\mathcal{M}_m}$  is injective and hence  $|Z_m| = |\pi(\mathcal{M}_m)| = |\mathcal{M}_m|$ .

Now set  $u = k/c$  and  $v = k(c-1)/c$  and define  $G := V \rtimes \mathbf{Z}_c(W)$ . Clearly,  $u + v = k$ . As  $G \leq W$ , for  $c > 0$ ,  $G$  is a nilpotent transitive group of degree  $p^k$  and nilpotency class at most  $c$ . Moreover,

$$|G| \geq |\mathbf{Z}_c(W)| \geq |Z_{c-1}| = |\mathcal{M}_{c-1}| \geq p^{u \binom{v}{c-1}} = p^{\frac{k}{c} \binom{k(c-1)/c}{c-1}}$$

and the first part of the proposition is proved.

Finally, for  $c = o(k)$ , we have

$$\frac{k}{c} \binom{k(c-1)/c}{c-1} = \frac{(c-1)^{c-1}}{c^c(c-1)!} k^c + o(k^{c-1})$$

and the second part is also proved.  $\square$

We conclude tabulating some values for  $\log_2(F_{\text{Nil}}(2^k, c))$  which can be obtain with the computer algebra system **magma** [2].

$k \backslash c$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	3	5	6	7	7	7	7	7	7	7	7	7	7	7	7	7
4	4	8	10	12	13	14	14	15	15	15	15	15	15	15	15	15
5	5	11	17	19	22	25	26	27	28	29	29	30	30	30	30	31

TABLE 2. Some values for  $\log_2(F_{\text{Nil}}(2^k, c))$

## REFERENCES

- [1] Y. Berkovich, *Groups of Prime Power Order Volume 1*, Walter de Gruyter, Germany, 2008.
- [2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.
- [3] J. D. Dixon, The Fitting subgroup of a linear solvable group, *J. Austral. Math. Soc.* **7** (1967), 417–424.
- [4] G. A. Fernández-Alcober, An introduction to finite  $p$ -groups: regular  $p$ -groups and groups of maximal class, Escola de Álgebra XVI, Brasília, 2000. <http://www.mat.unb.br/>
- [5] P. Lakatoš, V. Ī. Suščans'kiĭ, The coincidence of central series in wreath products I, *Publ. Math. Debrecen* **23** (1976), 167–176.
- [6] P. Pálffy, Estimates for the order of various permutation groups, *Contributions to General Algebra 12: Proceedings of the Vienna Conference*, June 3–6, 1999, Verlag Johannes Heyn, Klagenfurt 2000, 37–49.
- [7] P. Potočník, P. Spiga, G. Verret, Bounding the order of the vertex-stabiliser in 3-valent vertex-transitive and 4-valent arc-transitive graphs. arXiv:1010.2546v1 [math.CO].
- [8] P. Spiga, Elementary abelian  $p$ -groups of rank greater than or equal to  $4p - 2$  are not CI-groups, *J. Algebr. Comb.* **26** (2007), 343–355.
- [9] P. Spiga, G. Verret, On the order of vertex-stabilisers in vertex-transitive graphs with local group  $C_p \times C_p$  or  $C_p \text{ wr } C_2$ . arXiv:1311.4308 [math.CO].

ELEONORA CRESTANI, DIPARTIMENTO DI MATEMATICA, UNIVERSITY OF PADOVA, VIA TRIESTE 63, 35131 PADOVA, ITALY

*E-mail address:* `crestani@math.unipd.it`

PABLO SPIGA, DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITY OF MILANO-BICCOCÀ, VIA COZZI 55, 20125 MILANO, ITALY

*E-mail address:* `pablo.spiga@unimib.it`